INTENDER: Fuzzing Intent-Based Networking with Intent-State Transition Guidance

Jiwon Kim¹, Benjamin E. Ujcich², and Dave (Jing) Tian¹
¹Purdue University ²Georgetown University
USENIX Security 2023
“Allow access from marketing team to database via load balancer.”
“Allow access from marketing team to database via load balancer.”

Network-level Intent(s):
- SRC: MKT
- DST: DB
- Waypoint: LB
Compilation

Network-level Intent(s)

- SRC: MKT
- DST: DB
- Waypoint: LB

Network Object(s)

```
config {
  service: db.aa.com
  vip: DB
  port: 3306
  backends: [DB1, 2, 3]
}
```

<table>
<thead>
<tr>
<th>IN</th>
<th>SRC</th>
<th>DST</th>
<th>OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MKT1</td>
<td>DB</td>
<td>LB</td>
</tr>
<tr>
<td>2</td>
<td>MKT2</td>
<td>DB</td>
<td>LB</td>
</tr>
</tbody>
</table>
Activation

```
config {
  service: db.aa.com
  vip: DB
  port: 3306
  backends: [DB1, 2, 3]
}
```

<table>
<thead>
<tr>
<th>IN</th>
<th>SRC</th>
<th>DST</th>
<th>OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MKT1</td>
<td>DB</td>
<td>LB</td>
</tr>
<tr>
<td>2</td>
<td>MKT2</td>
<td>DB</td>
<td>LB</td>
</tr>
</tbody>
</table>

Network Object(s)

Control Plane

Data Plane

Network Devices
Monitoring

Telemetry Data

[S1] RX/TX
MKT1: 20mbps/20kbps
MKT2: 980mbps/20kbps
LB: 40kbps/1gbps

Control Plane

Data Plane

Network Devices
Verification

Telemetry Data

Result

INSTALLED,
98% Traffic from MKT2

[S1] RX/TX
MKT1: 20mbps/20kbps
MKT2: 980mbps/20kbps
LB: 40kbps/1gbps
Optimization

Summary

INSTALLED, 98% Traffic from MKT2

Result

In S1, 98% of traffic to LB comes from MKT2
“Allow access from marketing team to database via load balancer without congestion.”
Intent-Based Networking

- Translation
- Compilation
- Activation

Optimization
Verification
Observation

Intent State Machine

- REQ
- COMPILING
- INSTALLING
- INSTALLED
- FAILED
- REMOVED
Vulnerabilities in SDN and IBN

- Google’s B4 (2013)
- ODL (2014)
- ONOS with IBN (2016)
- ODL IBN (2017)
- Cisco DNAC (2020)
- ONAP IBN (2021)
- Google’s Orion (2021)

Cumulative CVEs:
- SDN
- IBN

Timeline:
- 2008
- 2013
- 2014
- 2016
- 2017
- 2020
- 2021
- 2022
- 2023H1
Fuzzing Programs

Fuzzer → Random Input → Target Program

Feedback

Coverage

Crash
Fuzzing IBN [1/3]
I. Bug Study in ONOS IBN

- Semantic
- Syntactic

61%

- Inconsistent State
- Connection Failure
- Garbage Rules
- Impact on Intents
I. Bug Study in ONOS IBN

Semantic bugs often do not cause program crashes

→ We need domain-specific detection methods
Fuzzing IBN [2/3]

Many Semantic Bugs
II. Limitation in Input Generation

Intent-Based Networking

Translation
Optimization
Compilation
Verification
Activation
Observation

\[ A \leftrightarrow B \]

Alice
Bob

Intent-Based Networking

Translation
Optimization
Compilation
Verification
Activation
Observation

\[ A \leftrightarrow B \]

Carol
David
II. Limitation in Input Generation

The success of an intent depends on the network. → We need topology-aware input generation.
Fuzzing IBN [3/3]

Many Semantic Bugs
III. Limitation in Code-Coverage Guidance

Case 1: INS-INS-DEL
- INSTALL x 2
- DELETE x 1
- COMPILE x 2
- DELETE x 1
- FLOW_ADD x 2
- FLOW_DEL x 1

Case 2: INS-DEL-INS
- INSTALL x 2
- DELETE x 1
- COMPILE x 2
- DELETE x 1
- FLOW_ADD x 2
- FLOW_DEL x 1

Intent-Based Networking

API

Intent

Flow

Alice ↔ Bob

k or \( k' \)

Case 1: INS-INS-DEL

Case 2: INS-DEL-INS

k

k'

k

k'

k

k'

A ↔ B

A ↔ B

k'

A ↔ B
III. Limitation in Code-Coverage Guidance

Code coverage cannot differentiate two cases

The order of operations (intent-state changes) matters

Case 1: INS-INS-DEL
Case 2: INS-DEL-INS

 INSTALL x 2
 DELETE x 1
 FLOW_ADD x 2
 FLOW_DEL x 1
Limitations in Fuzzing IBN

* Multiple-Operation Support: C/U/D & Topology Change

** Black-box Approach

New Coverage Metric for Feedback

Many Semantic Bugs
Intender: Fuzzing IBN

Intent-based State Transition Guidance (ISTG)

Topology-Aware Intent Generator (TAIG)

Black-box Approach

Multiple-Operation Support with Intent-Operation Dependency (IOD)

Detecting Syntactic and Semantic Bugs
**Intent-State Transition Guidance (ISTG)**

1. **Get seed**

2. **Mutate based on IOD/TAIG**

3. **Execute action**

4. **Read intent state**

5. **Record all transitions**

6. **Store scenario with new transitions**

---

**Intent-Transition History**

<table>
<thead>
<tr>
<th>Action</th>
<th>INSTALL</th>
<th>MODIFY</th>
<th>INSTALL</th>
<th>INSTALL</th>
<th>add-link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>F</td>
<td>I</td>
</tr>
<tr>
<td>Final</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
</tbody>
</table>
Evaluation (1/2)

- Environment Setup
  - Google Cloud VM: 4 vCPU, 16GB MEM, 60GB SSD
  - ONOS v2.5.1

- Found **12 new bugs (11 security-critical CVEs)**
  - 9 semantic bugs
  - Security impacts: network-wide *denial of service & tampering*

- Compare 4 existing fuzzers (AFL, Jazzer, Zest, PAZZ)
  - Up to **2.2×** better in branch coverage
  - Up to **82.6×** more number of unique errors
Evaluation (2/2)

• Improve fuzzing performance compared to baselines
  • *Topology-Aware Input Generation* (TAIG) can produce \(78.7\times\) more valid intents
  • *Intent-Operation Dependency* (IOD) can reduce 73.02\% of redundant operations
  • *Intent-State Transition Guidance* (ISTG) leads to \(1.8\times\) more intent-state transitions than code coverage guidance (CCG)
Case Study: CVE-2022-24035

(1) Eve requests **PURGE on INSTALLED intent**

![Diagram of Intent Manager and Pending Requests]

**Intent Manager**
- API Handlers
- Batch & Process

**Objective Tracker**
- Topology Change Handler

**Pending Requests**
- Wrong request remains in Pending because of bug.

**Current Intents**
- k

**ONOS Controller**

**Data Plane Network**

Eve requests PURGE on INSTALLED intent.
Case Study: CVE-2022-24035

(2) Eve exploits link-flooding attack

 Intent Manager
 API Handlers
 Batch & Process
 Topology Change Handler

 Intent Store
 Pending Requests
 Current Intents

② Intent should be recompiled if the path goes invalid.

Eve

\[ \text{Link Down} \]

ONOS Controller
Data Plane Network

Eve exploits link-flooding attack.
Case Study: CVE-2022-24035

(3) Intent **DOES NOT** respond to topology event any more → **DoS**⚠️

Eve

Intent Manager
- API Handlers
- Batch & Process

Objective Tracker
- Topology Change Handler

Intent Store
- Pending Requests
  - $k$
- Current Intents
  - $k$

3. Topology event is ignored to wait Pending request.

Data Plane Network

A

B

LINK DOWN

CVE!
Case Study: CVE-2022-24035

(3) Intent **DOES NOT** respond to topology event any more

- **To discover this bug efficiently…**

<table>
<thead>
<tr>
<th>Intent Transition History</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALL</td>
</tr>
<tr>
<td>PURGE</td>
</tr>
<tr>
<td>del-link</td>
</tr>
</tbody>
</table>

![Diagram showing the flow of intent processing and the issue with topology change handling.](image-url)
Conclusions

- Analyzed **186 bugs** in ONOS IBN
- Designed **new fuzzing techniques for IBN**
  - Topology-Aware Intent Generation (**TAIG**)  
  - Intent-Operation Dependency (**IOD**)  
  - Intent-State Transition Guidance (**ISTG**)  
- Developed **Intender architecture**
- Found **12 new bugs (11 CVEs)** in ONOS IBN
Thank you!

EMAIL  WEBSITE  CODE